IW610x

SESIP Security Target

Rev. 1.0 — 26 March 2025 **Evaluation document**

Document information

Information	Content
Keywords	SESIP, Security Target, Radio Co-Processor, IW610x
Abstract	Evaluation of the IW610x developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2), based on SESIP methodology, version 1.2.

Revision History

Rev.	Date	Description
1.0	26 March 2025	Initial release

1 Introduction

The IW610x device is a highly integrated dual WiFi and Bluetooth base-band used as a generic Radio Co-Processor (RCP) to be associated with a host processor to establishes secure communications with other devices in Thread networks (see https://www.threadgroup.org/).

The current SESIP Security Target (ST) defines the security services implemented by IW610x and assessed following the SESIP methodology [1], at the level.

In this Security Target, the table below provides some specific definitions to define the evaluation scope:

Table 1. Current ST scope terms definition

SESIP generic terms	Current ST specific definition
Platform	Platform is the evaluation scope; in this case IW610x, including its hardware and firmware.
Application	Application is out of the evaluation scope; it includes the host processor associated to IW610x, and the other devices of the network potentially direclty communicating with IW610x (not via the host processor).

1.1 ST Reference

IW610x, SESIP Security Target, Revision 1.0, NXP Semiconductors, 26 March 2025.

1.2 Platform Reference

IW610x has several variants detailed in chapters 1 (Table 1) and 2 (Table 3) of [4], depending on the combination of RF interfaces. All variants listed are in scope.

Table 2. Platform Reference

Reference	Value
Platform identification	IW610x v1.0 (x depend on radio configuration described in Table 1 and Table 3 of [4])
Platform version details	IW610x hardware: A1 IW610x Narrow band firmware: 2B122205 IW610x Wi-Fi firmware: 18.99.5.p43 Those versions correspond to the details provided in Section 3.2.1
Platform Type	Radio Co-Processor (RCP) with integrated WiFi, Bluetooth LE, 802.15.4 Tri-Radio

1.3 Other conformance claim

1.3.1 RED conformance claim

IW610x is compliant to the requirements from DIRECTIVE 2014/53/EU, Article 3 for radio equipments [10]. In particular, the following requirements are fulfilled by IW610x:

- Requirement 3.3 (d): radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- Requirement 3.3 (e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
- Requirement 3.3 (f): radio equipment supports certain features ensuring protection from fraud;

1.3.2 NIST 8425 conformance claim

IW610x fulfills the requirements from NIST 8425 [9] for IoT products. Please note that, the platform is not strictly in the scope of NIST 8425 because it is not an end product. Rather, the platform should be programmed with an OEM firmware and integrated with a host device to become an end product. Nevertheless, it is claimed that the platform meets all the requirements mandated by NIST 8425 and this shall directly contribute to the end product being fully compliant to NIST 8452.

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 3. Guidance Documents

Document	Reference
SESIP Security Target	IW610x, SESIP Security Target, Revision 1.0, NXP Semiconductors, 26 March 2025.
Datasheet	IW610x - 1x1 Wi-Fi 6 and Bluetooth Low Energy/802.15.4 Solution Family [4]
User Manual	UM12083 - Wi-Fi Software User Manual for IW610x [5]
User Manual	UM12082 - Bluetooth LE Software User Manual for IW610x [6]
User Manual	UM12084 - Bluetooth Low Energy (LE) HCI Software User Manual for IW610x [7]
User Manual	UM12088 - OpenThread Software User Manual for IW610x [8]
Application Note	AN13538 - Embedded Wi-Fi Subsystem API Specification V18 [3]

1.5 Platform Overview and Description

1.5.1 Platform Security Features and scope

The IW610x family is a highly integrated low-power single-chip solution with Wi-Fi 6 + Bluetooth Low Energy (LE) 5.4 / 802.15.4 radios designed for a broad array of applications. Applications include imaging, connected smart home devices, smart accessories, smart energy, enterprise industrial, and building automation RCP module is intended to be associated to a host processor as a basis for wireless communications between this host processor and other external devices.

IW610x security features in the scope of the evaluation are the following:

- Immutable Root of Trust
- Secure unique identification (version, type, instance)
- Secure life-cycle management
- Secure boot
- Secure update
- Secure communications with the network
- Signature based authenticated debug

The platform consists of hardware and firmware components represented on the figure below:

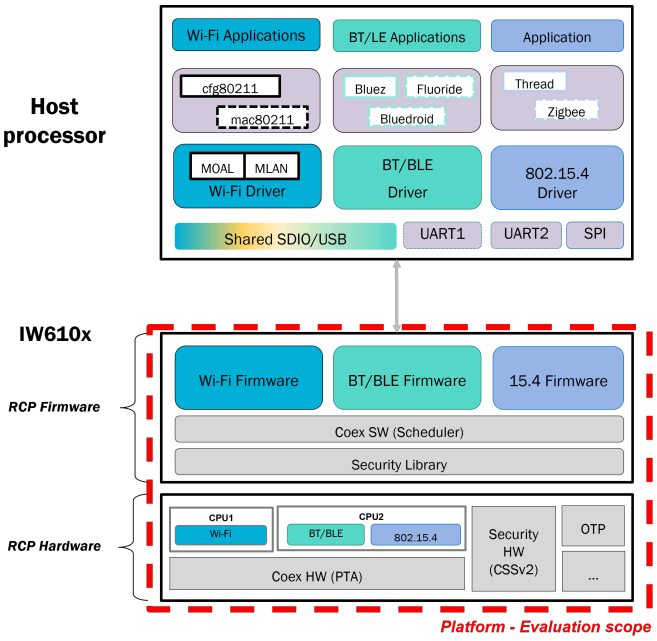

Figure 1. IW610x evaluation scope

The platform includes the following components and interfaces:

Table 4. Hardware and software components and interfaces

Components	Hardware components/interfaces	Software components/interfaces
WiFi	CPU 1 - Arm Cortex M3 and dedicated hardware (e.g. memories) Communication port WiFi 6E Host interfaces: SDIO 3.0, USB 2.0	BootROM and FW APIs 802.11 a/b/g/n/ax protocol APIs SDI, USB protocol APIs
BT/BLE	CPU 2 - Arm Cortex M3 and dedicated hardware (e.g. memories) Communication port Bluetooth 5.3 and BLE Host interfaces: UART1	BootROM and FW APIs 802.15.4 protocol APIs UART protocol APIs
15.4	CPU 2 (see BT/BLE) Communication port 802.15.4 Host interfaces: SPI	BootROM and FW APIs 802.15.4 protocol APIs SPINEL protocol APIs
Coex	Coex Hardware GPIOs+	WCI-2, PTA signals
Others	OTP controller PUF	

More details on IW610x components are provided in chapter 1 of [4]

1.5.2 Required Non-Platform Hardware/Software/Firmware

The platform is self-sufficient to be used as a RCP module.

Note that, for a final use into a Thread network, the platform is meant to be associated with a host processor implementing a Thread Host.

1.5.3 Life Cycle

The IW610x module implements a life-cycle based on states on which depends device security services (e.g. debug and test mode availability, asset accessibility).

The life-cycle is carefully secured:

- The state is stored in OTP fuse which can only be modified to reach the next step by burning additional bits; previous state can never be reached.
- The state is monotonic, it can only be increased which means that previous state can never be reached again.
- The state is checked during secure boot by the ROM, which determines the remaining boot flow, which operational mode to reach and which access to grant (e.g. debug).

More details about the life-cycle secure handling are provided in chapters 1.2 and 5 of [2]).

1.5.4 Use Case Environments

IW610x is a generic RCP module, therefore its final usage is not known. However, the next paragraphs describe the covered environmental conditions.

Logical access

The device is fully closed meaning that no feature allows the loading of untrusted code into IW610x. Therefore, logical accesses to IW610x resources are restricted by the external physical interfaces. Therefore, there is no logical boundary to be protected by isolation mechanism.

Physical access

IW610x is not intended to be protected against physical attacks. Therefore, if the final device operates in a public environment, the platform customer may need to put in place protections against physical attacks covering the IW610x security services, or to provide usage security guidelines to the final product owners.

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

For the platform to fulfill its security requirements, the operational environment (technical or procedural) must fulfil the following objectives:

Table 5. Platform Objectives for the Operational Environment

Title	Description
Platform Acceptance	When receiving the IW610x module, the integrator is expected to verify the correct version of all platform components that it depends on, as described in Section 3.2.1 section of this document.
Platform secure use	The integrator is expected to correctly and securely integrate and use the IW610x module in a Thread device by following all guidance part of the documentation listed in Section 1.4. In particular, the manufacturing and calibrating guidance must be applied first. Note that there is no different role or privilege.
Sensitive operations management	Sensitive operations to be handled by the environment as signature of firmware update must be done securely and by trusted actors.
Cryptographic material management	Cryptographic material as keys and certificates handled outside of the platform must be to securely handled by the environment.
Environmental conditions	If the IW610x module is to be used in a public environemnt, the integrator or final product vendor are responsible for the implementation of relevant security measures base on a risk analysis for the final use.

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP Assurance Level 2 (SESIP2)** as defined in Chapter 4 of Security Evaluation Standard for IoT Platforms (SESIP) [1].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

In accordance with the requirement for flaw reporting procedures (ALC_FLR.2), the developer has defined the following procedure:

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes four major steps:

- **Reporting**. The process begins when the PSIRT becomes aware of a potential security vulnerability in an NXP product. The reporter receives an acknowledgment and updates throughout the handling process.
- **Evaluation**. The PSIRT confirms the potential vulnerability, assesses the risk, determines the impact and assigns a processing priority. If the vulnerability is confirmed, the priority determines how the issue is handled throughout the remaining steps in the process.
- **Solution**. Working with PSIRT, the product team develops a solution that mitigates the reported security vulnerability. Solutions will take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM -, very often the solution can only be provided in a next version of the chips and the short-term solution will consist of recommending security measures to be applied in systems using the NXP product.
- **Communication**. As said above, because of the nature of the NXP products, the solution to systems using the affected products often needs to be found in additional countermeasures in those systems. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers. For previously unknown or unreported issues, NXP will acknowledge the reporter of the issues (unless the reporter requests otherwise).

The platform's secure boot mechanism is able to verify the authenticity of loadable firmwares and to update those as described in Section 3.2.4.

3.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

3.2.1 Verification of Platform Identity

Requirement

The platform provides a unique identification of the platform, including all its parts and their versions.

Refinement

Assets and protections related to this SFR are:

Table 6. Verification of platform identity assets

Asset	Protection required	Comments
RCP Identity – type and version	Integrity	The modification of the platform ID can impact the user proper identification of the RCP module in the overall system it is integrated to.

Conformance rationale

The unique identity is composed of the following parts:

Table 7. Verification of platform identity assets

Component	Identification command	Expected value
Wi-Fi hardware and firmware	Field *SysInfo* of APCMD_SYS_INFO command as described in [3].	ae 80 2a 00 30 10 00 00 **69 77 36 31 30 xx 2d 56 30 2c 20 53 44 49 4f 2c 20 46 50 39 39 2c 20 31 38 2e 39 39 2e 35 2e 70 34 33** *Device type: iw610x* (x depends of radio configuration described in Table 1 and Table 3 of [4]) *Revision number: V0* *HW information: SDIO or USB, FP99* *FW version number: 18.99.5.p43*
BLE/BT/802.15.4 hardware and firmware	Field *Events* of HCI_CMD_READ_FIRMWARE_REVISION command as described in [7].	01 0F FC 00 **05 22 12 2B 00 00 02 04** 00 *Firmware version: 2B122205* *ROM version: 04020000*

3.2.2 Verification of Platform Instance Identity

Requirement

The platform provides a unique identification of that specific instantiation of the platform, including all its parts.

Refinement

Assets and protections related to this SFR are:

Table 8. Verification of platform identity assets

Asset	Protection required	Comments
RCP Identity – instance unique ID	Integrity	The modification of the platform ID can impact the user proper identification of the RCP module in the overall system it is integrated to.

Conformance rationale

The platform stores in OTP fuses a 128-bit IETF RFC4122 compliant non-sequential Universally Unique Identifier (UUID). It can be read through the bring-up process for Wi-Fi interface via USB host interface described in chapter 2.2. of [5].

The unique identification of the platform can also be checked physically on the package as described in chapter 12.4 of [4] and marking in scope are listed in chapter 2 Table 3.

3.2.3 Secure Initialization of Platform

Requirement

The platform ensures its integrity and authenticity during platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to *standby state*.

Refinement

Assets and protections related to this SFR are:

Table 9. Secure initialization of platform assets

Asset	Protection required	Comments
RCP firmware	Integrity, authenticity	Firmware running on RCP. Modification of this asset would allow the attacker full control of the RCP; this could lead to attacks against the host processor and subsequently against the overall network. This could also lead to directly get access to RCP sensitive data (configuration values, trimming settings, counters) which could lower down or deactivate security mechanism, and/or to network credentials which could lead to access system network and consequently damaging malfunction of this system.

Conformance rationale

WiFi and BLE/802.15 services are executed on two different CPUs booting independently, both following the same secure boot process relying on a secure enclave.

The secure boot process gives access to different execution modes, the download mode, the boot sleep patch mode and the operational mode.

The secure enclave checks the integrity (SHA-256/384) and the authenticity (ECDSA P-256/384) of the firmware. The same public key is used for the Firmwares checking on both CPUs, and is stored in the firmware container header. The certificate can be revoked in case of corruption.

Firmware images are stored externally in containers and loaded from several hosts (e.g. SDIO, SPI, UART, USB, etc.), therefore their confidentiality is protected by and AES-128/256 CBC based encryption; their decryption is also handled by the secure enclave. Only a firmware successfully verified can be run and access the platform resources, protecting this way user data and network credentials.

In case the firmware verifications fail, the platform goes to a standby state i.e. a state in which the platform is waiting to be reset by the host.

In-field patches can only be loaded as part of a firmware container and are then protected by same mechanisms. Note that bootROM and secure enclave cannot be patched.

More details on secure boot are provided in [2]

3.2.4 Secure Update of Platform

Requirement

The platform can be updated to a newer version in the field such that the *confidentiality,* integrity and authenticity of the platform is maintained.

Refinement

Assets and protections related to this SFR are:

Table 10. Secure update of platform assets

Asset	Protection required	Comments
RCP firmware	Integrity, authenticity	Firmwares running on the RCP module.

Table 10. Secure update of platform assets*...continued*

Asset	Protection required	Comments
		Modification of this asset would allow the attacker full control of the RCP; this could lead to attacks against the host processor and subsequently against the overall network. This could also lead to directly get access to the RCP sensitive data (configuration values, trimming settings, counters) which could lower down or deactivate security mechanism, and/ or to network credentials which could lead to access system network and consequently damaging malfunction of this system.
RCP firmware version	Anti-rollback	Firmwares can only be updated to a version greater or equal to the current version. Rollback to a previous version could lead to load a vulnerable RCP firmware version, enabling attacks against RCP sensitive data and network credentials (see RCP firmware).

Conformance rationale

The secure update of IW610x follows the firmware download flow part of the secure boot during which the firmwares, and potentially patches, are checked as described in Section 3.2.3).

Anti-rollback of firmware is ensured by the comparison of the version embedded with the firmware and a reference version stored in OTP. Only a firmware version greater or equal to the OTP reference version is accepted.

More details on firmware downloading and patching are provided in the secure boot chapter of [2]

3.2.5 Secure Communication Support - RCP-Network

Requirement

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates *the endpoints listed in the table below* and protects against *the attacks listed in the table below* of messages between the end points, using *the protocols and measures listed below*.

Table 11. Secure communication RCP-Host selections

End point	Attacks to be protected against	Protocols and measures
Network devices	Disclosure, modification, replay, erasure	WiFi, BT/BLE, 802.15.4 protocols

Refinement

Assets and protections related to this SFR are:

Table 12. Secure communication RCP-Network assets

Asset	Protection required	Comments
Secure channel cryptographic material	Confidentiality, Integrity, authenticity	Cryptographic material to open and use a secure channel between the platform and remote network devices. The disclosure, modification or replacement of such material could lead to access sensitive data exchanged through the secure channel i.e. the network credential (Wifi/BLE/802.15.4 session keys) ensuring the protection of user data exchanged with other network devices.

Conformance rationale

The security of communications protocols between other network devices and the IW610x relies on the correct implementation of the WiFi, BT/BLE and 802.15.4 protocols as described in chapter 3 and 4 of [4].

The cryptographic material involved in secure channels establishment is protected by a secure key management relying on the RoT as described in [2]. As IW610x platform is a full dedicated and close device, no access to cryptographic material is possible by design.

3.2.6 Secure Debugging

Requirement

The platform only provides *JTAG interface* authenticated as specified in *[2]* with debug functionality.

The platform ensures that all data stored, with the exception of *None*, is made unavailable.

Refinement

All other assets and protections defined in Base SFRs can be impacted by access to debug feature and must be protected.

Conformance rationale

The CPU1 and CPU2 JTAG are locked when delivered to the customer. Access can only be unlocked, upon customer request, by the production of a specific firmware by NXP.

Details about secure debug are described in [2].

3.2.7 Availability support

Requirement

The platform ensures the availability and proper operation of *the Security Functional Requirements listed in the table below* for these following situations *listed in the table below*.

Table 13. Availability support selections

SFR	Situations
Secure communications	The host has required the sending of data to the network.

Refinement

None – no particular asset (out of the code itself) which could lead to break this SFR is identified.

Conformance rationale

The availability of software execution is supported by two watchdog mechanisms:

- A watchdog timer to reset the platform if the software does not respond within a time window;
- A hardware code watchdog for fault attacks or execution of unexpected instruction sequences.

Those two watchdogs are detailed in [2]

4 Mapping and Sufficiency Rationales

4.1 SESIP2 Sufficiency

Table 14. SESIP2 Sufficiency

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the platform reference in Section 1.2 and the platform overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Security Requirements and Implementation	All SFRs in this ST are taken from [1]. SFR "Identification of Platform Type" and SFR "Secure Update of Platform" are included.
	ASE_TSS.1 TOE Summary Specification	Security Requirements and Implementation	All SFRs are listed per definition, and for each SFR the implementation and rational are provided in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Material provided to the evaluator	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

4.2 Conformance mapping for RED

The table below shows how the platform under evaluation, IW610x, described in this Security Target supports the RED compliance ([10]); it describes which part of each RED requirements are implemented at the IW610x own level. Then, this is the responsibility of the device to use the security features described to implement the final requirement.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of end device compliance demonstration to RED standard.

Table 15. RED security requirements support by IW610x

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by IW610x and assessed by SESIP
ACM-1	Applicability of access control mechanisms	d/e/f	Not applicable: the RCP has logical interfaces with the host processor only and does not requires access control.
ACM-2	Appropriate access control mechanisms	d/e/f	Same as above
ACM-3	Default access control for children in toys	e	Same as above
ACM-4	Default access control to children's privacy assets for toys and childcare equipment	e	Same as above
ACM-5	Parental/Guardian access controls for children in toys	e	Same as above
ACM-6	Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	e	Same as above
AUM-1	Applicability of authentication mechanisms	d/e/f	Same as above
AUM-2	Appropriate authentication mechanisms	d/e/f	Same as above
AUM-3	Authenticator validation	d/e/f	Same as above
AUM-4	Changing authenticators	d/e/f	Same as above
AUM-5	Password strength	d/e/f	Same as above
AUM-5	Password strength	d/e/f	Same as above
AUM-6	Brute force protection	d/e/f	Same as above
SUM-1	Applicability of update mechanisms	d/e/f	Section 3.2.4 Section 3.1.1
SUM-2	Secure updates	d/e/f	Same as above
SUM-3	Automated updates	d/e/f	Not applicable: the RCP update triggering, and then automaticity, is under the responsibility of the host processor.
SSM-1	Applicability of secure storage mechanisms	d/e/f	Not applicable: the RCP does not store persistently device or network security assets.
SSM-2	Appropriate integrity protection for secure storage mechanisms	d/e/f	Same as above
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	d/e/f	Same as above

Table 15. RED security requirements support by IW610x*...continued*

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by IW610x and assessed by SESIP
SCM-1	Applicability of secure communication mechanisms	d/e/f	Section 3.2.5
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	d/e/f	Same as above
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	d/e/f	Same as above
SCM-4	Appropriate replay protection for secure communication mechanisms	d/e/f	Same as above
LGM-1	Applicability of logging mechanisms	e/f	Not applicable: the RCP does not handle privacy nor finantial assets, and therefore does not require related logging mechanisms.
LGM-2	Persistent storage of log data	e/f	Same as above
LGM-3	Minimum number of persistently stored events	e/f	Same as above
LGM-4	Time-related information of persistently stored log data	e/f	Same as above
DLM-1	Applicability of deletion mechanisms	e	Not applicable: the RCP does not handle personal data nor sensitive security parameters, and therefore does not require deletion mechanism.
RLM-1	Applicability of resilience mechanisms	d	Section 3.2.3 Section 3.2.7
NMM-1	Applicability of and appropriate network monitoring mechanisms	d	Not applicable: the RCP has no direct interactions with the network, and therefore cannot monitor any network activity.
TCM-1	Applicability of and appropriate traffic control mechanisms	d	Not applicable: the RCP has no direct interactions with the network, and therefore cannot control any network traffic.
UNM-1	Applicability of user notification mechanisms	e	Not applicable: the RCP does not handle any end-user information and has no direct interaction with this one, and therefore does not directly notify the end-user.
UNM-2	Content of user notification)	e	Same as above
CKK-1	Appropriate CCKs	d/e/f	Section 3.2.5

Table 15. RED security requirements support by IW610x*...continued*

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by IW610x and assessed by SESIP
CCK-2	CCK generation mechanisms	d/e/f	Same as above
CCK-3	Preventing static default values for preinstalled CCKs	d/e/f	Same as above
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	d/e/f	This is checked by the SESIP AVA_VAN evalaution activity.
GEC-2	Limit exposure of services via related network interfaces	d/e/f	Same as above
GEC-3	Configuration of optional services and the related exposed network interfaces	d/e/f	Not applicable: the RCP has no interfaces exposed via network interfaces affecting security assets or network assets.
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	d/e/f	This is required and checked by the AGD_PRE and AGD_OPE SESIP evaluation activities.
GEC-5	No unnecessary external interfaces	d/e/f	This is checked by the SESIP AVA_VAN evalaution activity.
GEC-6	Input validation	d/e/f	Same as above
GEC-7	Documentation of external sensing capabilities	e	Not applicable: the RCP does not implement any external sensing capabilities.
GEC-8	Equipment Integrity	f	Section 3.2.3
CRY-1	Best practice Cryptography	d/e/f	Section 3.2.3 Section 3.2.4 Section 3.2.5 Section 3.2.6

4.3 Conformance mapping for NIST 8425

The table below shows how the platform under evaluation, IW610x, described in this Security Target supports the final IoT device (as defined in the NIST 8425 [9]; component of the IoT product), to show compliance with the NIST 8425 security requirements; it describes which part of each NIST 8425 requirements are implemented at the IW610x own level. Then, this is the responsibility of the device to use the security features described to implement the final requirement.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of end device compliance demonstration to NIST 8425 standard.

NIST 8425 defines the IoT product as a system made of components like IoT device(s), mobile application(s), backend web application(s). In this context, the mapping provided below only holds for the IoT device.

Table 16. NIST 8425 security requirements support by IW610x

NIST 8425 requirements	IW610x supports
Asset Identification	
1. The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).	Verification of Platform Identity supports the IoT device to be uniquely identified by providing a unique and tamper-proof identification of the type and version of its IW610x subcomponent. Verification of Platform Instance Identity supports the IoT device to be uniquely identified by providing a tamper-proof identity of its IW610x subcomponent, and unique per IoT device instances.
2. The IoT product uniquely identifies each IoT product component and maintains an up-to- date inventory of connected product components.	
Product Configuration	
1. Authorized individuals (i.e., customer), services, and other IoT product components can change the configuration settings of the IoT product via one or more IoT product components.	The authorization and configuration of the IoT device, as part of an IoT IoT product, shall be implemented by the operating system or application code. However, the platform can support through the Secure Update of Platform feature which allows the IoT device to update to a newer version in the field in secure manner if this is needed for a configuration update.
2. Authorized individuals (i.e., customer), services, and other IoT product components have the ability to restore the IoT product to a secure default (i.e., uninitialized) configuration.	The authorization and configuration of the IoT device, as part of an IoT product, shall be implemented by the operating system or application code.
3. The IoT product applies configuration settings to applicable IoT components.	The configuration of the IoT device, as part of an IoT product, shall be implemented by the operating system or application code. However, the platform can support through the Secure Update of Platform feature which allows the IoT device to update the configuration settings of its IW610x subcomponent, as well as other processors of the SoC, to a newer version in the field in a secure manner if this is needed for a configuration update.
Data Protection	
1. Each IoT product component protects data it stores via secure means	The platform following features protect the IoT device data stored by the IW610x subcomponent: Secure Debugging supports the secure data storage by protecting unauthorized access to those data via debug features. Secure Initialization of Platform and Secure Update of Platform ensure the authenticity and integrity of the code and then indirectly he expected access restrictions to the confidential data already stored.
2. The IoT product has the ability to delete or render inaccessible stored data that are either collected from or about the customer, home, family, etc.	No data collected by or abou the customer related information is handled by the IW610x subcomponent. This shall be implemented by upper layer handling such data.
3. When data are sent between IoT product components or outside the product, protections are used for the data transmission.	The communication function of the IoT device, as part of an IoT product, shall be fully facilitated by the operating system or application code.
Interface Access Control	
1. Each IoT product component controls access to and from all interfaces (e.g., local interfaces, whether externally accessible or	The design of final IoT device, as part of an IoT product, including the physical interface exposure and its

Table 16. NIST 8425 security requirements support by IW610x*...continued*

NIST 8425 requirements	IW610x supports
not, network interfaces, protocols, and services) in order to limit access to only authorized entities. At a minimum, the IoT product component shall: a. Use and have access only to interfaces necessary for the IoT product's operation. All other channels and access to channels are removed or secured. b. For all interfaces necessary for the IoT product's use, access control measures are in place (e.g., unique password-based multifactor authentication, physical interface ports inaccessible from the outside of a component). c. For all interfaces, access and modification privileges are limited.	usability, is by the platform integrator. The access control, authentication, and communcation mechanism shall also be implemented by the operating system or application code. For the access to the IW610x subcomponent interfaces: Secure Debugging supports the access control to the IW610x interfaces by protecting unauthorized access to those interfaces in debug mode. Also, the AVA (vulnerability analysis), ADV (development) and ATE (functional testing) activities in SESIP evaluation verify that the interfaces provided at IW610x level are restricted to only the necessary functions and privileges, and there is no unnecessary privilege, interface and/or code remained.
2. Some, but not necessarily all, IoT product components have the means to protect and maintain interface access control. At a minimum, the IoT product shall: a. Validate that data shared among IoT product components match specified definitions of format and content. b. Prevent unauthorized transmissions or access to other product components. c. Maintain appropriate access control during initial connection (i.e., onboarding) and when reestablishing connectivity after disconnection or outage.	
Software Update	
1. Each IoT product component can receive, verify, and apply verified software updates.	Secure Update of Platform implements the secure update of the IW610x subcomponent ensuring integrity and authentication verification. The software update development, distribution and customer notification are expected to be managed by platform integrator and/or the network service providers.
2. The IoT product implements measures to keep software on IoT product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via the IoT product).	
Cybersecurity State Awareness	
1. The IoT product securely captures and records information about the state of IoT components that can be used to detect cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.	The cybersecurity state awareness of the IoT device, as part of an IoT product, shall be designed and implemented by the operating system or application code. All SESIP SFRs support the components to provide the capability to manage audit records relevant to security by outputing status which can be integrated to the component audit records.
Documentation	
The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.	NXP creates and stores documents related to the IW610x cybersecurity all along its development and its subsequent lifecycle. The ASE (Security Target) SESIP evaluation activities (see [1]) ensures that information is provided related to expected use case and security scope (like assurance level, assumptions on the operational environment, security functionalities,etc...) of the IW610x subcomponent

Table 16. NIST 8425 security requirements support by IW610x*...continued*

NIST 8425 requirements	IW610x supports
	The AGD (Guidance) SESIP evaluation activities (see [1]) ensures that information is provided related to secure use of the IW610x subcomponent.
Information and Query Reception	
The IoT product developer has the ability to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.	This requirement primarily address the platform integrators and/or the network service providers. NXP also provides a flaw reporting procedure for its products. Flaw Reporting Procedure (ALC_FLR.2) SESIP evaluation activities (see also [1]) support the IoT device developer to respond to user queries about information relevant to cybersecurity by requiring for the IW610x subcomponent, the implementation and the assessment of a flaw remediation process.
Information Dissemination	
The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.	This requirement primarily address the platform integrators and/or the network service providers. NXP also distributes information relevent to cybersecurity to its customer. The ASE (Security Target) and AGD (user guidance) SESIP evaluation activities (see [1]) support the IoT device developer disseminating information relevant to cybersecurity by providing information needed related to the IW610x subcomponent. Flaw Reporting Procedure (ALC_FLR.2) SESIP evaluation activities (see also [1]) support the IoT device developer to respond to user queries about information relevant to cybersecurity by requiring for the IW610x subcomponent, the implementation and the assessment of a flaw remediation process.
Product Education and Awareness	
The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.	This requirement primarily addresses the platform integrators and/or the network service providers. NXP also distributes information relevent to cybersecurity to its customer. The ASE (Security Target) and AGD (user guidance) SESIP evaluation activities (see [1]) support the IoT device developer disseminating information relevant to cybersecurity by providing information needed related to the IW610x subcomponent. Flaw Reporting Procedure (ALC_FLR.2) SESIP evaluation activities (see also [1]) support the IoT device developer to respond to user queries about information relevant to cybersecurity by requiring for the IW610x subcomponent, the implementation and the assessment of a flaw remediation process.

5 Bibliography

5.1 Evaluation Documents

[1] Security Evaluation Standard for IoT Platforms (SESIP), GlobalPlatform GP_FST_070, version 1.2.

5.2 Developer Documents

[2] Nighthawk Security Architecture Manual, NXP Semiconductors, rev. 0.2
[3] AN13538 - Embedded Wi-Fi Subsystem API Specification V18 , NXP Semiconductors, rev. 2
[4] IW610x - 1x1 Wi-Fi 6 and Bluetooth Low Energy/802.15.4 Solution Family, NXP Semiconductors, rev.3
[5] UM12083 - Wi-Fi Software User Manual for IW610x, NXP Semiconductors, rev.1
[6] UM12082 - Bluetooth LE Software User Manual for IW610x, NXP Semiconductors, rev.1
[7] UM12084 - Bluetooth Low Energy (LE) HCI Software User Manual for IW610x, NXP Semiconductors, rev.1
[8] UM12088 - OpenThread Software User Manual for IW610x, NXP Semiconductors, rev.1

5.3 External Documents

[9] NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products, National Institute of Standards and Technology, September 2022
[10] EN 18031 Common security requirements for radio equipment, , April 16 2024

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents